CLAIMS

Now, therefore, the following is claimed:

1. A system for securely transmitting data messages, comprising:

a first computer configured transmit a data message, said data message having a header and a data portion, said first computer configured to encrypt said data portion via a first encryption technique and to encrypt said header via a second encryption technique, said first computer further configured to include information associated with said first encryption technique in said header; and

a second computer configured to receive said first data message and to decrypt said header, said second computer further configured to decrypt said data portion based on said information included in said header.

2. The system of claim 1, wherein said information associated with said first encryption technique identifies said second encryption technique.

3. The system of claim 1, wherein said second encryption technique includes RSA encryption.

4. The system of claim 3, wherein said first encryption technique includes DES encryption.

5. The system of claim 1, wherein said first computer transmits a public key to said second computer, and wherein said second computer utilizes said public key to decrypt said header.

6. The system of claim 5, wherein said first computer is configured to encrypt said public key before transmitting said public key to said second computer.

7. The system of claim 1, wherein said information associated with said first encryption technique identifies an encryption key used by said first computer to encrypt said data portion.

8. The system of claim7, wherein said first computer randomly selects said encryption key.

9. The system of claim 1, wherein said second computer is configured to transmit a list of encryption techniques to said first computer and said first computer is configured to select said first encryption technique from said list.

10. The system of claim 9, wherein said first computer randomly selects said first encryption technique from said list.

11. A system for transmitting messages, comprising:

means for defining a data portion of a data message;

means for encrypting said data portion via a first encryption technique;

means for defining a header of said data message, said header including information associated with said first encryption technique;

means for encrypting said header via a second encryption technique; and

means for transmitting said message.

12. A method for transmitting messages, comprising the steps of:

defining a data portion of a first data message;

encrypting said data portion of said first data message via a first encryption technique;

defining a header of said first data message, said header of said first data message including information associated with said first encryption technique;

encrypting said header of said first data message via a second encryption technique; and

transmitting said first data message subsequent to said encrypting steps.

13. The method of claim 12, further comprising the steps of:

receiving a list of encryption techniques; and

randomly selecting said first encryption technique from said list.

14. The method of claim 12, wherein said first encryption technique includes RSA encryption.

15. The method of claim 14, wherein said second encryption technique includes DES encryption.

16. The method of claim 12, wherein said encrypting said data portion step includes the step of encrypting said data portion of said first data message with an encryption key, said method further comprising the step of including said encryption key in said header of said first data message.

17. The method of claim 16, further comprising the step of randomly selecting said encryption key.

18. The method of claim 12, further comprising the steps of:

receiving said first data message transmitted in said transmitting step;

decrypting said header of said first data message; and

decrypting said data portion of said first data message based on said information included in said header of said first data message.

19. The method of claim 18, further comprising the step of identifying said first encryption technique via information included in said header of said first data message.

20. The method of claim 18, further comprising the steps of:

transmitting a public key; and

decrypting said header of said first data message based on said public key.

21. The method of claim 20, further comprising the step of encrypting said public key before said transmitting a public key step.

22. The method of claim 12, further comprising the steps of:

defining a data portion of a second data message;

encrypting said data portion of said second data message via a third encryption technique;

defining a header of said second data message, said header of said second data message including information associated with said third encryption technique;

encrypting said header of said second data message via said second encryption technique; and

transmitting said second data message.

23. The method of claim 22, further comprising the step of randomly selecting said first and third encryption techniques.

24. The method of claim 23, further comprising the steps of:

receiving said second message;

decrypting said header of said second message; and

decrypting said data portion of said second message based on said information included in said header of said second message.